

Chiamate URI SIP Jabber su MRA

Sommario

[Introduzione](#)

[Scenario](#)

[Presupposti](#)

[Configurazione sull'organizzazione 1 quando Jabber A chiama Jabber B](#)

[Il flusso complessivo delle chiamate in uscita diventa](#)

[Configurazione sull'organizzazione 1 quando Jabber B chiama Jabber A](#)

[Il flusso complessivo delle chiamate in entrata diventa](#)

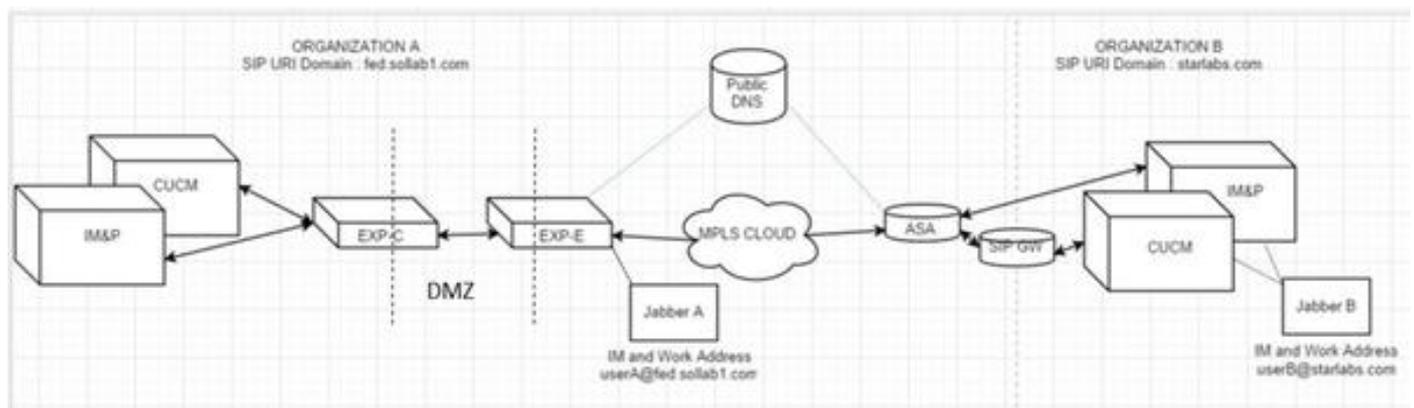
Introduzione

In questo documento viene descritta la configurazione di Cisco Unified Communications Manager (CUCM) ed Expressway C ed E in modo che jabber possa chiamare l'URI (Uniform Resource Identifier) del protocollo SIP (Session Initiation Protocol) di un altro utente di un'organizzazione diversa quando connesso tramite MRA (Mobile Remote Access). Lo stesso nel contesto di Expressway è anche chiamato flusso di chiamata B2B.

Scenario

Si supponga che l'organizzazione 1 distribuisca l'ARR e l'organizzazione 2 no. Per l'organizzazione 2, il perimetro termina con un'appliance ASA (Adaptive Security Appliance), oltre la quale è presente CUBE che è integrata con il cluster CUCM dell'organizzazione 2.

Come mostrato nell'immagine, Jabber A può essere connesso tramite MRA o internamente, ma la configurazione rimane la stessa su CUCM, Expressway C ed E, per l'organizzazione 1.



Presupposti

Si può supporre che gli utenti Jabber A e Jabber B siano in grado di scambiare messaggi

istantanei e informazioni sulla presenza tramite la federazione XMPP (Extensible Messaging and Presence Protocol) e che i relativi indirizzi IM siano anche gli URI SIP per il lavoro.

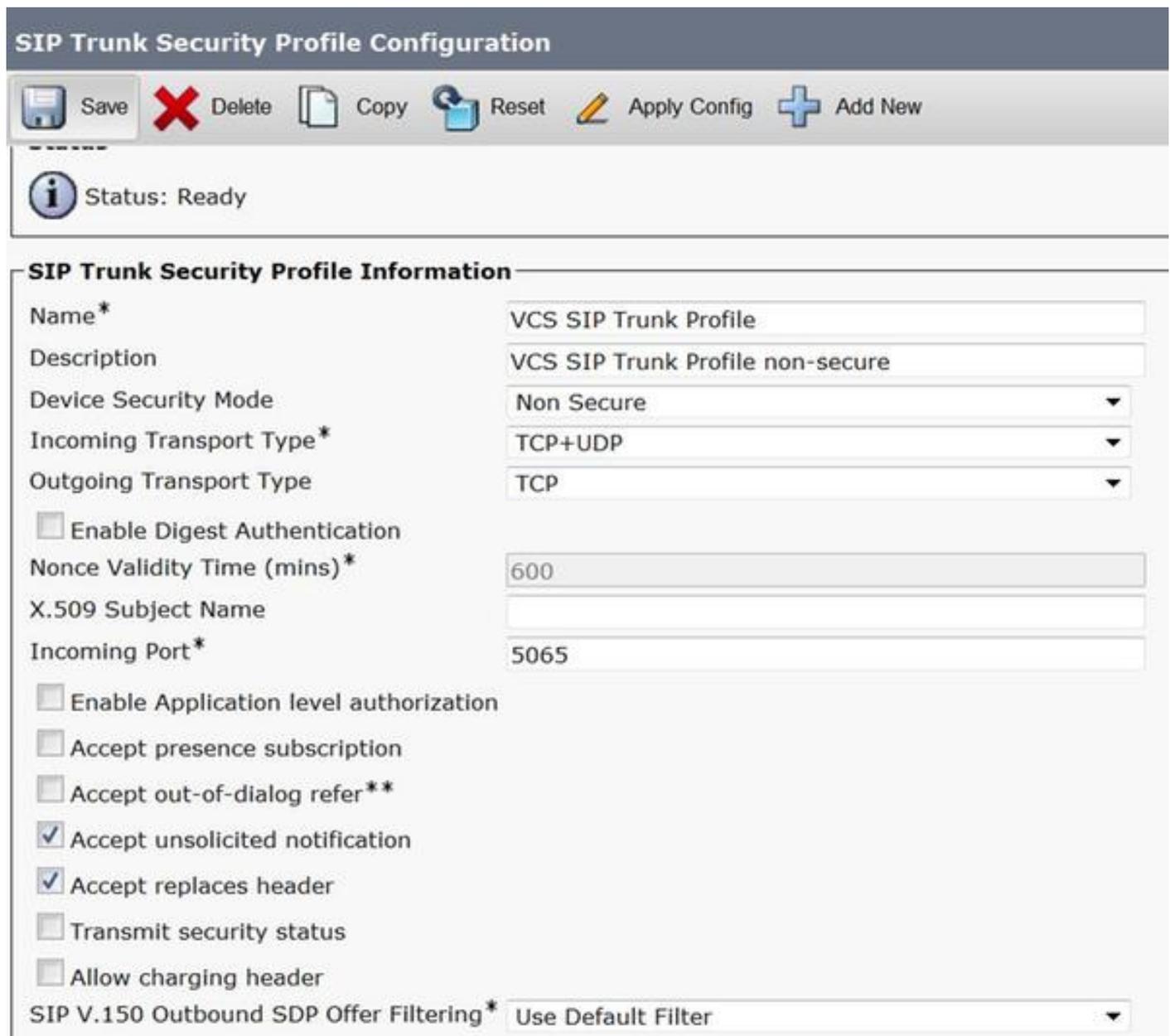
Inoltre, Jabber A e Jabber B sono in grado di comporre tramite SIP URI internamente, all'interno delle rispettive organizzazioni, con successo.

Nello scenario precedente, si presuppone che l'organizzazione 2 abbia CUCM come server di controllo delle chiamate. Tuttavia, può anche essere un server di controllo delle chiamate di un altro fornitore.

È necessario conoscere la versione durante l'integrazione di CUCM, Jabber, VCS per MRA.

Configurazione sull'organizzazione 1 quando Jabber A chiama Jabber B

Passaggio 1. Creare un nuovo profilo SIP Trunk Security, con una porta di attesa di 5065, come mostrato nell'immagine:



SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status: Ready

SIP Trunk Security Profile Information

Name*	VCS SIP Trunk Profile
Description	VCS SIP Trunk Profile non-secure
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5065
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

Passaggio 2. Creare un trunk SIP che punti a ExpressWay-C e assegnare il profilo SIP Trunk Security, come mostrato nell'immagine:

SIP Information

-Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.106.82.114		5060

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* VCS SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard SIP Profile For Cisco VCS [View Details](#)

DTMF Signaling Method* RFC 2833

-Normalization Script

Nota: Viene creato un nuovo profilo Trunk Security che resta in ascolto sulla porta 5065. Viene assegnato a questo nuovo trunk SIP che punta a Expressway-C perché Expressway-C è già configurato per inviare le registrazioni non sicure di Jabber su 5060 a CUCM quando l'utente Jabber accede tramite MRA. Se si utilizza il profilo predefinito Trunk Security, il jabber connesso tramite MRA non riesce a registrarsi sulla porta 5060 di CUCM.

Passaggio 3. Creare il modello di route SIP per l'URI dell'organizzazione 2 e assegnarlo al punto di trunk SIP a Expressway-C, come mostrato nell'immagine:

SIP Route Pattern Configuration

 Save  Delete  Copy  Add New

Status

 Status: Ready

Pattern Definition

Pattern Usage Domain Routing

IPv4 Pattern* starlabs.com

IPv6 Pattern

Description VCS MRA calls

Route Partition < None >

SIP Trunk/Route List* VCS-MRA-TRNK

Block Pattern

Passaggio 4. Creare una zona adiacente su Expressway-C che punti a CUCM, come mostrato nell'immagine:

The image shows a configuration interface for Cisco Expressway-C, divided into three sections: Configuration, H.323, and SIP. Each section has a title bar and a list of settings.

- Configuration**
 - Name: CUCM-ORG1
 - Type: Neighbor
 - Hop count: 15
- H.323**
 - Mode: Off
- SIP**
 - Mode: On
 - Port: 5065
 - Transport: TCP
 - Accept proxied registrations: Deny
 - Media encryption mode: Auto
 - ICE support: Off

Passaggio 5. Creare una zona client trasversale su Expressway-C (non UC Traversal), come mostrato nell'immagine:

EDIT 2016

Type	Traversal client
Hop count	★ 15 ⓘ

Connection credentials

Username	★ cisco ⓘ
Password	★ ●●●●●●●● ⓘ

H.323

Mode	Off ⓘ
------	-------

SIP

Mode	On ⓘ
Port	★ 7003 ⓘ
Transport	TCP ⓘ
Accept proxied registrations	Allow ⓘ
Media encryption mode	Auto ⓘ
ICE support	Off ⓘ
SIP noison mode	Off ⓘ

Passaggio 6. Creare una zona server trasversale su Expressway-E (non UC Traversal), come mostrato nell'immagine:

Edit zone

Type	Traversal server
Hop count	15 <input type="text"/>
Connection credentials	
Username	cisco <input type="text"/>
Password	Add/Edit local authentication database
H.323	
Mode	Off <input type="text"/>
SIP	
Mode	On <input type="text"/>
Port	7003 <input type="text"/>
Transport	TCP <input type="text"/>
Accept proxied registrations	Allow <input type="text"/>
Media encryption mode	Auto <input type="text"/>
ICE support	Off <input type="text"/>
...	Off <input type="text"/>

Passaggio 7. Creare una zona DNS in Expressway-C, da utilizzare per eseguire una ricerca DNS SRV dell'URI dell'organizzazione 2, come mostrato nell'immagine:

Configuration	
Name	★ VCS-MRA-DNS ⓘ
Type	DNS
Hop count	★ 15 ⓘ

H.323	
Mode	Off ▼ ⓘ

SIP	
Mode	On ▼ ⓘ
TLS verify mode	Off ▼ ⓘ
Fallback transport protocol	UDP ▼ ⓘ
Media encryption mode	Auto ▼ ⓘ
ICE support	Off ▼ ⓘ

Una volta create tutte le zone, è necessario definire le regole di ricerca su Expressway C ed E in modo da poter eseguire il routing.

Passaggio 8. La regola di ricerca in Expressway-C prevede l'inoltro dell'invito **SIP** destinato all'URI starlabs.com a Expressway-E sulla nuova zona di attraversamento creata, come mostrato nell'immagine:

Configuration	
Rule name	★ Inside-to-Outside-MRA-CUCMORG2 ⓘ
Description	ⓘ
Priority	★ 99 ⓘ
Protocol	SIP ▼ ⓘ
Source	Any ▼ ⓘ
Request must be authenticated	No ▼ ⓘ
Mode	Alias pattern match ▼ ⓘ
Pattern type	Regex ▼ ⓘ
Pattern string	★ .*@starlabs.com\$ ⓘ
Pattern behavior	Leave ▼ ⓘ
On successful match	Continue ▼ ⓘ
Target	★ b2b ▼ ⓘ
State	Enabled ▼ ⓘ

Passaggio 9. Regola di ricerca su Expressway-E per inoltrare l'invito SIP destinato all'URI starlabs.com a DNS ZONE dopo che la chiamata ha raggiunto Expressway-E via la zona trasversale, come mostrato nell'immagine:

Rule name	CUCM to VCSe to DNS
Description	VCS MRA calls
Priority	130
Protocol	SIP
Source	Named
Source name	b2b
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	*.starlabs.com\$
Pattern behavior	Leave
On successful match	Continue
Target	VCS-MRA-DNS
State	Enabled

Passaggio 10. Dopo che la chiamata ha raggiunto la zona DNS, Expressway-C esegue una ricerca DNS SRV per `_sips.tcp.starlabs.com`, `_sip._tcp.starlabs.com` e `_sip._udp.starlabs.com` sul server DNS pubblico.

Nei log Exp-E, è possibile visualizzare quanto segue:

```
2016-03-09T09:48:35+05:30 VCSECOL tvcs: UTCTime="2016-03-09 04:18:35,399" Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="_sip._tcp.starlabs.com" Type="SRV (IPv4 and IPv6)"
```

```
2016-03-09T09:48:35+05:30 VCSECOL tvcs: UTCTime="2016-03-09 04:18:35,400" Module="network.dns" Level="DEBUG": Detail="Resolved hostname to: ['IPv4''TCP''14.160.103.10:5060'] (A/AAAA) Number of relevant records retrieved: 1"
```

Dalla ricerca DNS SRV, Exp-E ottiene l'IP e la porta per l'hop successivo, per raggiungere l'organizzazione 2. In questo scenario, DNS SRV `_sip._tcp.starlabs.com` si risolve nel FQDN/IP pubblico e nella porta 5060 dell'ASA per l'organizzazione 2.

Il flusso complessivo delle chiamate in uscita diventa

1. Jabber A compone `userB@starlabs.com` come URI SIP.
2. L'invito SIP raggiunge CUCM (tramite Exp-E → Exp-C).
3. CUCM esegue l'analisi delle cifre che corrisponde al modello di route SIP.
4. CUCM instrada la chiamata a Exp-C tramite SIP Trunk.

5. Exp-C riceve la chiamata sulla 'zona adiacente CUCM' e la 'regola di ricerca' inoltra la chiamata alla zona attraversante che è stata effettuata.
6. Call now raggiunge Exp-E tramite la "zona trasversale" e la regola di ricerca inoltra la chiamata alla "zona DNS".
7. Una volta raggiunta la zona DNS, DNS SRV cerca `_sip._tcp.starlabs.com` rispetto al server DNS pubblico, che si risolve all'hop successivo per raggiungere l'organizzazione 2.

Configurazione sull'organizzazione 1 quando Jabber B chiama Jabber A

Si supponga ora che l'organizzazione 2 disponga di un proprio piano di composizione configurato per instradare una chiamata URI SIP all'organizzazione 1, quando Jabber B chiama Jabber A. Per ottenere l'invito SIP in arrivo, vedere le modifiche necessarie, instradare a CUCM dell'organizzazione 1.

Passaggio 1. Regola di ricerca in ingresso su Expressway-E, per l'invio di un invito SIP in ingresso dall'organizzazione 2 a Exp-C, per il dominio URI SIP **fed.sollab1.com**, come mostrato nell'immagine:

The image shows a configuration page for a search rule. The left sidebar lists various configuration fields, and the right side shows the corresponding values for a rule named 'VCS to VCS to CUCM'. The rule is set to priority 120, protocol SIP, source Any, and mode Alias pattern match. The pattern type is Regex with the string `.*@fed.sollab1.com$`. The pattern behavior is set to 'Leave' and the action on successful match is 'Continue'. The target is 'b2b' and the rule is currently 'Enabled'.

Field	Value
Rule name	VCS to VCS to CUCM
Description	VCS MRA calls from outside
Priority	120
Protocol	SIP
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	.*@fed.sollab1.com\$
Pattern behavior	Leave
On successful match	Continue
Target	b2b
State	Enabled

Passaggio 2. Regola di ricerca in ingresso su Expressway-C, per l'invio di un invito SIP in ingresso da Exp-E a CUCM, per il dominio URI SIP **fed.sollab1.com**, come mostrato nell'immagine:

Configuration	
Rule name	★ Outside-to-Inside-MRA
Description	VCS MRA calls from outside
Priority	★ 98 ⓘ
Protocol	SIP ⓘ
Source	Named ⓘ
Source name	★ b2b ⓘ
Request must be authenticated	No ⓘ
Mode	Alias pattern match ⓘ
Pattern type	Regex ⓘ
Pattern string	★ .*@fed.sollab1.com\$ ⓘ
Pattern behavior	Leave ⓘ
On successful match	Continue ⓘ
Target	★ CUCM-ORG1 ⓘ
State	Enabled ⓘ

Il flusso complessivo delle chiamate in entrata diventa

1. Inbound SIP INVITE from Jabber B for **userA@fed.sollab1.com** hits Exp-E.
2. La regola di ricerca su Exp-E inoltra la chiamata a Exp-C tramite la "zona trasversale".
3. Regola di ricerca su Exp-C , inoltra la chiamata al cluster CUCM tramite la 'Zona adiacente CUCM'.
4. CUCM invia l'invito SIP a Jabber A registrato su MRA (tramite Exp-C → Exp-E).

Nota: Per il corretto funzionamento delle chiamate B2B, sono necessarie licenze per i rich media sia su Expresssway-C che su Expresssway-E.

Nota: Verificare che le porte aperte sul firewall siano corrette.